KONINKRIJK DER NEDERLANDEN

Bureau voor de Industriële Eigendom

Hierbij wordt verklaard, dat in Nederland op 12 maart 1999 onder nummer 1011544,

ten name van:

KONINKLIJKE KPN N.V.

te Groningen

een aanvrage om octrooi werd ingediend voor:

"Werkwijze en inrichting voor het cryptografisch bewerken van data",

onder inroeping van een recht van voorrang, gebaseerd op de in Nederland op 30 december 1998 onder nummer 1010921 ingediende aanvrage om octrooi, en

dat de hieraan gehechte stukken overeenstemmen met de oorspronkelijk ingediende stukken.

Rijswijk, 1 oktober 1999.

De Directeur van het Bureau voor de Industriële Eigendom,
voor deze,

A.W. van der Kruk

1011544
18

UITTREKSEL

Bij het cryptografisch bewerken van data worden deze data (X) en een sleutel (K) aan een cryptografisch proces (P) toegevoerd, dat een bekend proces kan zijn. Teneinde de aard van het proces (P) te versluieren worden aan het proces hulpwaarden toegevoerd, zoals een aanvullende sleutel (K*), met behulp waarvan een aanvullend proces (P*) de eigenlijke sleutel (K) genereert. De combinatie van het oorspronkelijke proces (P) en het aanvullende proces (P*) levert een onbekend proces op, waarbij de relatie tussen de aanvullende sleutel (K*) en de bewerkte data (Y) onbekend is. Hierdoor wordt een betere cryptografische beveiliging verkregen.

(Fig. 2)

7-II

985240/RBE/KFA

Korte aanduiding: Werkwijze en inrichting voor het cryptografisch bewerken van data.

ACHTERGROND VAN DE UITVINDING

De uitvinding heeft betrekking op een werkwijze voor het cryptografisch bewerken van data, omvattende het aan een cryptografisch proces toevoeren van waarden, te weten de data en een sleutel, en het uitvoeren van het proces teneinde cryptografisch bewerkte data te vormen. Een dergelijke werkwijze is in de praktijk bekend.

Voor het cryptografisch bewerken van data worden in de praktijk vaak algemeen bekende processen toegepast. Voorbeelden van dergelijke cryptografische processen (algoritmen) zijn DES en RSA, die bijvoorbeeld zijn beschreven in het boek "Applied Cryptography" door B. Schneier (2e uitgave), New York, 1996.

Deze processen worden gepubliceerd omdat men ervan uitging dat het, bij een voldoende grote sleutellengte, ondoenlijk zou zijn aan de hand van de bewerkte data de oorspronkelijke data en/of de sleutel te achterhalen, ook al was het cryptografische proces bekend.

Recentelijk zijn echter aanvallen ontdekt die zijn gebaseerd op kennis van het cryptografische proces. Met andere woorden, doordat het gedrag van het proces bekend is wordt het, bij bepaalde aanvallen, aanzienlijk eenvoudiger om de gebruikte sleutel en/of de oorspronkelijke data te herleiden. Het zal duidelijk zijn dat dit ongewenst is.

SAMENVATTING VAN DE UITVINDING

De uitvinding beoogt bovengenoemd probleem op te lossen door een werkwijze en schakeling voor het uitvoeren van een cryptografisch proces aan te geven die het herleiden van de sleutel bij toepassing van een bekend (d.w.z. openbaar) cryptografisch proces aanzienlijk bemoeilijken of zelfs ondoenlijk maken. Een werkwijze van

de in de aanhef genoemde soort is hiertoe overeenkomstig de uitvinding gekenmerkt door het aan het proces toevoeren van hulpwaarden teneinde de in het proces gebruikte waarden te maskeren.

Door het maskeren van de data en/of sleutel(s) wordt het aanzienlijk moeilijker deze waarden aan de hand van het gedrag van het proces te herleiden. Het resultaat van het proces, dat wil zeggen de verzameling bewerkte data, kan bij een geschikte keuze van de hulpwaarden onveranderd zijn, dat wil zeggen identiek zijn aan het resultaat van het proces indien daar geen hulpwaarden aan zijn toegevoerd. In dit verband wordt onder een "hulpwaarde" een waarde (data of sleutel) verstaan, die in aanvulling op de corresponderende data en sleutel aan het proces wordt toegevoerd.

De uitvinding is derhalve gebaseerd op het inzicht, dat het herleiden van de in een cryptografisch proces gebruikte waarden aanzienlijk gecompliceerd wordt indien deze waarden door middel van hulpwaarden zijn gemaskeerd.

De uitvinding is mede gebaseerd op het verdere inzicht, dat het gebruik van hulpwaarden het resultaat van het proces niet noodzakelijkerwijs beïnvloedt.

In een eerste uitvoeringsvorm van de uitvinding omvat een hulpwaarde een aanvullende sleutel die aan een aanvullend proces wordt toegevoerd teneinde de sleutel te vormen.

Door een combinatie van een bekend proces en een aanvullend proces toe te passen wordt een nieuw, op zich onbekend cryptografisch proces gevormd, zelfs indien het aanvullende proces ook op zich bekend is.

Door de voor het bekende proces gebruikte sleutel (primaire sleutel) af te leiden uit een aanvullende sleutel (secundaire sleutel) met behulp van een aanvullend proces wordt bereikt dat niet de (primaire) sleutel van het bekende proces maar de aanvullende (secundaire) sleutel aan de combinatie van processen wordt aangeboden. Met andere woorden, extern wordt de aanvullende (secundaire)

sleutel en niet de werkelijke (primaire) sleutel van het eigenlijke proces gebruikt. Het afleiden van de sleutel uit de oorspronkelijke data en de bewerkte data is daarmee ondoenlijk geworden. Tevens is het afleiden van de aanvullende sleutel ernstig bemoeilijkt, omdat de combinatie van het oorspronkelijke proces en het aanvullende proces niet bekend is.

Deze uitvoeringsvorm van de uitvinding is derhalve onder meer gebaseerd op het inzicht, dat het bekend zijn van een cryptografisch proces ongewenst is, dit in tegenstelling tot wat tot dusver werd aangenomen. Deze uitvoeringsvorm is tevens gebaseerd op het verdere inzicht, dat aanvallen die voortbouwen op kennis van het proces aanzienlijk moeilijker worden indien het proces onbekend is.

Bij voorkeur omvat het aanvullende proces een cryptografisch proces. Dit maakt het herleiden van de aanvullende sleutel moeilijker. In principe kan echter bijvoorbeeld een eenvoudige codering als aanvullend proces worden toegepast. Bij een cryptografisch proces wordt bij voorkeur een hulpsleutel toegepast.

Met voordeel is het aanvullende proces een inverteerbaar proces. Dit maakt het mogelijk de werkwijze volgens de uitvinding bij bestaande apparatuur met minimale wijzigingen toe te passen. Indien bijvoorbeeld een eerste inrichting een (aanvullende) sleutel afgeeft die in een tweede inrichting overeenkomstig de uitvinding wordt toegepast, kan in de eerste inrichting de inverse van het aanvullende proces worden gebruikt om de aanvullende sleutel uit de oorspronkelijke sleutel af te leiden. Met andere woorden, hoewel in zowel de eerste als de tweede inrichting intern de oorspronkelijke (primaire) sleutel wordt gebruikt, wordt tussen de inrichtingen de aanvullende (secundaire) sleutel uitgewisseld. Het onderscheppen van de aanvullende sleutel leidt echter niet tot kennis van de oorspronkelijke sleutel.

Het kan voordelig zijn als het uitvoeren van het aanvullende proces uitsluitend plaatsvindt indien de data

vooraf bepaalde eigenschappen bezitten. Op deze wijze kan het cryptografisch bewerken alleen voor bepaalde, geselecteerde data worden uitgevoerd, terwijl dit voor alle andere data is geblokkeerd. Op deze wijze wordt een aanvullende bescherming bereikt.

Een optimale beveiliging wordt geboden indien het proces en het aanvullende proces elk uit een aantal stappen zijn opgebouwd, en waarin afwisselend stappen van het proces en het aanvullende proces worden uitgevoerd. Hierdoor worden de eigenschappen van het bekende proces verder versluierd, waardoor het herleiden van de sleutels verder wordt bemoeilijkt.

In een tweede uitvoeringsvorm van de uitvinding omvat het proces een aantal trappen met elk een cryptografische bewerking voor het bewerken van uit de data afgeleide rechter data en een combinatiebewerking voor het met uit de data afgeleide linker data combineren van de bewerkte rechter data teneinde gemodificeerde data te vormen, waarin de rechter data, voorafgaande aan de bewerking F, gecombineerd worden met een primaire hulpwaarde. Daardoor is het mogelijk de in de cryptografische bewerking gebruikte data te maskeren.

Bij voorkeur worden de bewerkte rechter data telkens gecombineerd met een secundaire hulpwaarde. Hierdoor is het onder meer mogelijk de gemodificeerde linker data te maskeren.

Met voordeel is de secundaire hulpwaarde van een trap gevormd uit de combinatie van de primaire hulpwaarde van de voorgaande trap en de primaire hulpwaarde van de volgende trap. Hierdoor wordt het mogelijk de hulpwaarde in de telkens volgende trap te compenseren, waardoor deze hulpwaarde niet in het eindresultaat van het proces zal doorwerken. Een verdere maskering van alle data, in het bijzonder in de eerste trap, wordt bereikt indien de primaire hulpwaarde van de eerste trap tevens met de linker data wordt gecombineerd.

Het is mogelijk de werkwijze volgens de uitvinding

zodanig uit te voeren, dat alle primaire hulpwaarden gelijk zijn. Hierdoor is een zeer eenvoudige praktische realisatie mogelijk. Het gebruik van verschillende hulpwaarden, die bij voorkeur toevalsgetallen zijn en voor elke keer dat het proces wordt uitgevoerd opnieuw worden gegenereerd, biedt echter een grotere cryptografische beveiliging.

Een verdere vereenvoudiging van deze uitvoeringsvorm kan worden verkregen indien de primaire hulpwaarden en/of secundaire hulpwaarden telkens vooraf met de respectieve bewerking zijn gecombineerd. Dat wil zeggen, het combineren met hulpwaarden wordt in de betreffende bewerking (bijvoorbeeld een substitutie) verwerkt, zodat het resultaat van de respectieve bewerking gelijk is aan dat van de oorspronkelijke bewerking plus een of twee combinatiebewerkingen met hulpwaarden. Door het vooraf in de bewerking opnemen van de combinatiebewerkingen is een eenvoudiger en snellere praktische realisatie mogelijk.

De genoemde combinatiebewerkingen worden bij voorkeur door middel van een exclusief-of-bewerking uitgevoerd. Andere combinatiebewerkingen, zoals binair optellen, zijn in principe echter ook mogelijk.

De uitvinding verschaft verder een schakeling voor het uitvoeren van een werkwijze voor het cryptografisch bewerken van data. De uitvinding verschaft bovendien een betaalkaart en een betaalterminal die van een dergelijke schakeling zijn voorzien.

De uitvinding zal in het onderstaande aan de hand van in de figuren weergegeven uitvoeringsvoorbeelden nader worden toegelicht.

KORTE BESCHRIJVING VAN DE TEKENINGEN

Fig. 1 toont schematisch een cryptografisch proces volgens de stand van de techniek.

Fig. 2 toont schematisch een eerste cryptografisch proces volgens een eerste uitvoeringsvorm van de uitvinding.

Fig. 3 toont schematisch een tweede cryptografisch proces volgens een eerste uitvoeringsvorm van de uitvinding.

Fig. 4 toont schematisch een wijze waarop de processen van Fig. 1 en 2 kunnen worden uitgevoerd.

Fig. 5 toont schematisch een eerste cryptografisch proces volgens een tweede uitvoeringsvorm van de uitvinding.

Fig. 6 toont schematisch een tweede cryptografisch proces volgens een tweede uitvoeringsvorm van de uitvinding.

Fig. 7 toont schematisch een derde cryptografisch proces volgens een derde uitvoeringsvorm van de uitvinding.

Fig. 8 toont schematisch een schakeling waarin de uitvinding wordt toegepast.

Fig. 9 toont schematisch een betaalsysteem waarin de uitvinding wordt toegepast.

VOORKEURSUITVOERINGSVORMEN

Een (cryptografisch) proces P volgens de stand van de techniek is in figuur 1 schematisch weergegeven. Aan het proces P worden ingangsdata X en een sleutel K toegevoerd. Aan de hand van de sleutel K zet het proces P de ingangsdata X om in (cryptografisch) bewerkte uitgangsdata Y: $Y = P_K(X)$. Het proces P kan een bekend cryptografisch proces zijn, zoals DES (Data Encryption Standard), drievoudige DES, of RSA (Rivest, Shamir & Adleman).

Indien de ingangsdata X en de uitgangsdata Y bekend zijn is het in principe mogelijk de gebruikte sleutel K te herleiden. Bij een sleutel met een voldoende grote lengte (d.w.z., een voldoend groot aantal bits) werd het tot nu toe ondoenlijk geacht deze sleutel te herleiden, zelfs indien het proces P bekend was. Ondoenlijk wil in dit geval zeggen dat het in theorie weliswaar mogelijk is, bijvoorbeeld door het proberen van alle mogelijke sleutels, om de gebruikte sleutel te achterhalen, maar

dat dit een onbruikbaar lange rekentijd vergt. Een dergelijke aanval met brute kracht ("brute force attack") is daarom nauwelijks een bedreiging voor de cryptografische beveiliging.

Recent ontdekte aanvallen maken echter gebruik van kennis van het proces, waardoor het aantal mogelijke sleutels drastisch kan worden gereduceerd. Het herleiden van de gebruikte sleutel K en/of de ingangsdata X uit de uitgangsdata Y wordt daardoor binnen aanvaardbare rekentijden mogelijk.

Het principe van de uitvinding, die beoogt dergelijke aanvallen aanzienlijk moeilijker en tijdrovender te maken, is in fig. 2 schematisch weergegeven. Evenals in fig. 1 worden aan een (bekend) proces P ingangsdata X en een (geheime) sleutel K toegevoerd om uitgangsdata Y te genereren.

In tegenstelling tot de situatie van fig. 1 wordt in de situatie van fig. 2 de sleutel K vanuit een aanvullend proces P* aan het proces P toegevoerd. Het aanvullende proces P* heeft een aanvullende (secundaire) sleutel K* als ingangsdata om, onder invloed van een hulpsleutel K', de (primaire) sleutel K als uitgangsdata te produceren. De sleutel K wordt dus niet, zoals in de situatie van fig. 1, vanuit een externe bron (bijvoorbeeld een geheugen) aan het proces P toegevoerd, maar wordt door het proces P* voortgebracht uit de aanvullende (secundaire) sleutel K*:

$$K = P^*_{K'}(K)$$

Het is dus de secundaire sleutel K* in plaats van de primaire sleutel K die vooraf is bepaald en die bijvoorbeeld in een sleutelgeheugen (niet getoond) wordt opgeslagen. Overeenkomstig de uitvinding is de primaire sleutel K die aan het proces P wordt toegevoerd niet vooraf bepaald.

De hulpsleutel K' kan een vast opgeslagen, vooraf bepaalde sleutel zijn. Het is ook mogelijk een aanvullend proces P* toe te passen waarin geen hulpsleutel K' wordt

gebruikt.

De combinatie van de processen P en P* vormt een nieuw proces, dat schematisch is aangeduid als Q. Aan het proces Q, dat vanwege het aanvullende proces P* op zich onbekend is, worden de ingangsdata X en de (secundaire) sleutel K* toegevoerd om de uitgangsdata Y te produceren. De relatie tussen de secundaire sleutel K* en de primaire sleutel K wordt door het aanvullende proces P* verslui-erd.

Het aanvullende proces P* is bij voorkeur de inverse van een ander, inverteerbaar proces R. Dat wil zeggen:

$$P^* = R^{-1}.$$

Dit maakt het mogelijk de secundaire sleutel K* met behulp van R en de hulpsleutel K' voort te brengen uit de primaire sleutel K:

$$K^* = R_{K'}(K),$$

zoals later aan de hand van figuur 5 nader zal worden toegelicht. Eventueel kan het nieuwe proces Q worden uitgebreid met het proces R, zodat de primaire sleutel K in plaats van de secundaire sleutel K* aan het proces Q wordt toegevoerd. De primaire sleutel K wordt in dat geval in het proces Q afgeleid uit:

$$K = P^*_{K'}(K^*) = P^*_{K'}(R_{K'}(K)).$$

Dit maakt het mogelijk dezelfde (primaire) sleutel te gebruiken als in de stand van de techniek.

Het in fig. 3 schematisch weergegeven cryptografische proces volgens de uitvinding omvat eveneens een proces P met een primaire sleutel K en een aanvullende proces P* met een hulpsleutel K', waarbij de primaire sleutel K door het aanvullende proces P* uit de aanvullende sleutel K* wordt afgeleid. In aanvulling op het proces van fig. 1 worden in dit geval ook de ingangsdata X aan het aanvullende proces P* toegevoerd, zodat de primaire sleutel K mede in afhankelijkheid van de ingangsdata X wordt bepaald:

$$K = P^*_{K'}(K^*, X)$$

Hierdoor wordt een aanvullende cryptografische be-

scherming gekregen. Bovendien wordt hierdoor de mogelijkheid geboden het aanvullende proces P* uitsluitend uit te voeren indien bepaalde ingangsdata worden aangeboden. Dat wil zeggen, het aanvullende proces P* kan een test van de ingangsdata X omvatten en het uitvoeren van het aanvullende proces P* kan afhangen van het resultaat van die test. Zo kan het aanvullende proces P* bijvoorbeeld slechts worden uitgevoerd als de laatste twee bits van de invoerdata X gelijk zijn aan nul. Het effect van een dergelijke ingangsdata-afhankelijke bewerking is, dat slechts voor bepaalde ingangsdata X de juiste primaire sleutel K zal worden geproduceerd, zodat alleen die ingangsdata de gewenste uitgangsdata Y opleveren. Het zal duidelijk zijn dat de cryptografische veiligheid hierdoor verder wordt vergroot.

In fig. 4 is schematisch de wijze weergegeven waarop deelstappen van de processen P en P* afwisselend kunnen worden uitgevoerd ("interleaving") teneinde de bescherming tegen aanvallen verder te vergroten. De deelstappen kunnen zogenaamde "rondes" omvatten, zoals bijvoorbeeld bij DES het geval is. Bij voorkeur omvatten de deelstappen echter slechts een of enkele instructies van een programma, waarmee de processen worden uitgevoerd.

In een eerste stap 101 wordt een eerste deelstap P_1 van het proces P uitgevoerd. Vervolgens wordt in een tweede stap 102 de eerste deelstap P_1* van het aanvullende proces P* uitgevoerd. Evenzo wordt in een derde stap 103 de tweede deelstap P_2 van het proces P uitgevoerd enz. Dit gaat door totdat in stap 110 de laatste deelstap P_n* van het aanvullende proces P* is uitgevoerd, waarbij omwille van het voorbeeld ervan is uitgegaan dat de processen P en P* evenveel deelstappen omvatten. Indien dat niet het geval is, wordt in stap 110 de laatste overeenkomstige deelstap uitgevoerd, en worden in verdere stappen de resterende deelstappen uitgevoerd.

Door het afwisselen van de deelstappen van het op zich bekende proces P en het (mogelijk eveneens op zich

bekende) proces P* kan een reeks van deelstappen worden verkregen, die niet overeenkomt met die van een bekend proces. De aard van het proces is hierdoor moeilijker te herkennen.

Het in fig. 5 schematisch weergegeven cryptografisch proces omvat een aantal trappen S (S_1, S_2, ...). In elke trap S worden (rechter) data RD toegevoerd aan een cryptografische bewerking F. Deze cryptografische bewerking kan zelf een aantal deelstappen omvatten, zoals een expansie, een combinatie met een sleutel, een substitutie en een permutatie. De cryptografische bewerking F levert bewerkte data RD', die in een combinatiebewerking CC (CC_1, CC_2, ..., de index geeft steeds de betreffende trap S aan) met linker data LD worden gecombineerd tot gemodificeerde (linker) data LD', die evenals de oorspronkelijke rechter data RD worden doorgegeven aan de volgende trap.

Zoals in fig. 5 is getoond, wisselen aan het eind van elke trap S de gemodificeerde linker data LD' en de rechter data RD van positie, zodat deze respectievelijk de rechter data RD en de linker data LD van de volgende trap vormen.

De linker data LD en de rechter data RD zijn in een voorafgaande bewerking PP afgeleid uit ingangsdata X en kunnen daarbij een voorbereidende permutatie ondergaan. De uitgangsdata van de laatste trap vormen de bewerkte data Y van de werkwijze, eventueel nadat deze een eindbewerking, zoals een uitgangspermutatie PP^{-1}, hebben ondergaan.

Overeenkomstig de uitvinding worden de in en tussen de trappen aanwezige data gemaskeerd met hulpwaarden. Zo is in elke trap, bijvoorbeeld de trap S_2, een aanvullende combinatiebewerking AC aanwezig die de rechter data RD combineert met een (primaire) hulpwaarde A voordat deze data aan de cryptografische bewerking F worden toegevoerd. Een verdere combinatiebewerking BC is tussen de cryptografische bewerking F en de combinatiebewerking CC ingevoegd met het doel de bewerkte (rechter) data RD' met

een verdere (secundaire) hulpwaarde B te combineren. Bij voorkeur zijn alle combinatiebewerkingen exclusief-of-bewerkingen.

Het combineren van de data LD en RD met de hulpwaarden A en B heeft tot gevolg, dat de gemodificeerde data LD' gemaskeerd zijn, waardoor het aanzienlijk moeilijker is de oorspronkelijke data LD en RD uit de gemaskeerde data LD' te herleiden.

Overeenkomstig een verder aspect van de uitvinding zijn de hulpwaarden A en B gerelateerd. De tweede hulpwaarde B is bij voorkeur door middel van een exclusief-of-bewerking gevormd uit de eerste hulpwaarde A_1 van de vorige trap en de hulpwaarde A van de volgende trap:

$$B_i = A_{i-1} \oplus A_{i+1}.$$

Dit heeft tot gevolg, dat elke hulpwaarde A die middels een verdere aanvullende combinatiebewerking BC als bestanddeel van de verdere hulpwaarde B met de rechter data RD is gecombineerd telkens in de volgende trap wordt gecompenseerd voordat de data aan de bewerking F worden onderworpen. De hulpwaarde A werkt echter wel door in de gemodificeerde data LD', zodat deze tussen twee trappen gemaskeerd blijven.

Met voordeel gaan aan de eerste trap S_1 voorbereidende combinatiebewerkingen EC en DC vooraf, die respectievelijk de rechter data RD_1 en de linker data LD_1 van de eerste trap S_1 vormen aan de hand van respectievelijk de primaire hulpwaarde A_1 van de eerste trap en een primaire hulpwaarde A_0. Deze combinatiebewerkingen zijn bij voorkeur ook exclusief-of-bewerkingen. In dat geval heeft de combinatiebewerking AC_1 het effect de hulpwaarde A_1 uit de rechter data RD_1 te verwijderen alvorens deze aan de bewerking F_1 worden aangeboden. In de rechter data RD_1, die door de kruislingse omwisseling in de tweede trap S_2 de linker data LD_2 gaan vormen, blijft de hulpwaarde A_1 en daarmee de maskering van de data behouden.

De tweede data SD_1 van de eerste trap S_1 zijn gemaskeerd met de additionele hulpwaarde A_0. Door het combine-

ren met de hulpwaarde $B_1 = A_0 \oplus A_2$ wordt de aanvankelijke hulpwaarde A_0 verwijderd (wegens $A_0 \oplus A_0 = 0$), maar blijft de hulpwaarde A_2 en de daarmee bereikte maskering behouden. De hulpwaarde A_0 wordt in deze uitvoeringsvorm bij voorkeur gelijk gekozen aan A_1.

Teneinde de hulpwaarden voorafgaand aan de eindbewerking (PP^{-1}) te verwijderen zijn afsluitende combinatiebewerkingen FC en GC voorzien, die de gemodificeerde linker data LD'_n van de laatste trap S_n met een hulpwaarde A_{n+1} respectievelijk de rechter data RD_n met een hulpwaarde A_n combineren. Hierdoor is het mogelijk de werkwijze zodanig uit te voeren, dat ondanks het gebruik van de hulpwaarden A de einddata Y gelijk zijn aan die welke met de conventionele werkwijze zouden zijn verkregen.

Hoewel bij voorkeur alle hulpwaarden A_i verschillend worden gekozen, met uitzondering van $A_0 = A_1$, is het mogelijk alle hulpwaarden A_i gelijk te kiezen. In dat geval zijn alle secundaire hulpwaarden in de weergegeven uitvoeringsvorm gelijk aan nul, zodat de verdere combinatiebewerkingen BC achterwege kunnen blijven.

In het proces van fig. 6, dat grotendeels overeenkomt met dat van fig. 5, zijn de combinatiebewerkingen AC en BC en de cryptografische bewerking F geïntegreerd tot een gecombineerde bewerking F'. Het integreren van de combinatiebewerkingen is mogelijk door bijvoorbeeld een substitutietabel van de bewerking F op geschikte wijze aan te passen. Hierdoor kunnen de aanvullende combinatiebewerkingen AC en BC achterwege blijven. In principe is voor elke trap S_i een verschillende gecombineerde bewerking F_i nodig, waarin verschillende hulpwaarden A_i zijn geïntegreerd (zie Fig. 5). Slechts indien de hulpwaarden A_i gelijk worden gekozen, d.w.z. $A_1 = A_2 = ... = A_n$, kunnen de gecombineerde bewerkingen F_i gelijk zijn.

De uitvoeringsvorm van fig. 7 komt grotendeels overeen met die van Fig. 6. In aanvulling op Fig. 6 is in elke trap S, met uitzondering van de laatste trap S_n, een combinatiebewerking HC opgenomen die de rechter data RD

met een tertiaire hulpwaarde W combineert. Bij voorkeur is de teriaire hulpwaarde gelijk aan de exclusief - of - combinatie van de hulpwaarden A_0 en A_1:

$$W = A_0 \oplus A_1.$$

Dit heeft het resultaat dat de bewerking HC steeds de hulpwaarde A_0 toevoegt en de hulpwaarde A_1 compenseert. Hierdoor is het mogelijk dat alle cryptografische bewerkingen F in wezen identiek zijn, hetgeen een veel geringere verwerkings- en/of opslagcapaciteit vereist van een processorsysteem waarmee de werkwijze wordt uitgevoerd. Het zal duidelijk zijn dat in de uitvoeringsvorm van Fig. 7 de bewerkingen F" zodanige aanpassingen van de oorspronkelijke bewerkingen F zijn, dat deze gecorrigeerd zijn voor de hulpwaarde A_1 en bovendien de hulpwaarde A_0 hun resultaat combineren. Met andere woorden, indien RD $\oplus$ A_1 aan F" wordt toegevoerd, is het resultaat gelijk aan F" (RD) $\oplus$ W.

In fig. 8 is schematisch een schakeling 10 voor het ten uitvoer leggen van de werkwijze volgens de uitvinding getoond. De schakeling 10 omvat een eerste geheugen 11, een tweede geheugen 12 en een processor 13, waarbij de geheugens 11 en 12 en de processor 13 door middel van een databus 14 zijn gekoppeld. Door het verschaffen van twee geheugens is het mogelijk telkens een deelstap van een van de processen P en P* uit te voeren (zie fig. 4), het resultaat van die deelstap in bijvoorbeeld het eerste geheugen 11 op te slaan, en vanuit het tweede geheugen 12 een vorig tussenresultaat van het andere proces naar de processor 13 over te brengen. Op deze wijze is het mogelijk het afwisselend berekenen van deelstappen van twee verschillende processen efficiënt uit te voeren.

Het in fig. 9 schematisch weergegeven betaalsysteem omvat een elektronisch betaalmiddel 1 en een betaalstation 2. Het elektronische betaalmiddel 1 is bijvoorbeeld een zogenaamde "smart card", d.w.z. een kaart die van een geïntegreerde schakeling voor het opslaan en verwerken van betaalgegevens is voorzien. Het betaalstation 2 omvat

een kaartlezer 21 en een processorschakeling 22. De processorschakeling 22 kan overeenkomen met de schakeling 10 van fig. 5.

Aan het begin van een transactie draagt het betaalmiddel 1 een identificatie (kaartidentificatie) ID over naar het betaalstation 2. Aan de hand van deze identificatie bepaalt het betaalstation 2 een sleutel die voor deze transactie zal worden gebruikt. Deze identificatie ID kan als ingangsdata X (zie de figuren 1-3) aan een cryptografisch proces worden toegevoerd dat aan de hand van een meestersleutel MK een identificatie-afhankelijke transactiesleutel K_{ID} als uitgangsdata Y produceert. Overeenkomstig de uitvinding wordt hiervoor het in de figuren 2 en 3 weergegeven proces gebruikt, waarbij de meestersleutel MK vooraf met behulp van een proces R is omgezet in een aanvullende meestersleutel MK*. Deze aanvullende meestersleutel MK* wordt nu, bij voorkeur samen met de identificatie ID overeenkomstig fig. 3, toegevoerd aan het aanvullende proces P* teneinde de oorspronkelijke meestersleutel MK te reproduceren en de transactiesleutel K_{ID} uit de identificatie ID af te leiden.

Hoewel in de figuren 2 en 3 steeds een enkel aanvullend proces P* is getoond, kunnen eventueel meerdere processen P*, P**, P***, ... in serie en/of parallel worden gebruikt om de primaire sleutel K af te leiden.

Het zal deskundigen duidelijk zijn dat vele wijzigingen en aanvullingen mogelijk zijn zonder buiten het kader van de uitvinding te treden.

CONCLUSIES

1. Werkwijze voor het cryptografisch bewerken van data, omvattende het aan een cryptografisch proces (P) toevoeren van waarden, te weten de data (X) en een sleutel (K), en het uitvoeren van het proces (P) teneinde cryptografisch bewerkte data (Y) te vormen, **gekenmerkt door** het aan het proces (P) toevoeren van hulpwaarden (K*; A, B) teneinde de in het proces (P) gebruikte waarden (K; D) te maskeren.

2. Werkwijze volgens conclusie 1, waarin een hulpwaarde een aanvullende sleutel (K*) omvat die aan een aanvullend proces (P*) wordt toegevoerd teneinde de sleutel (K) te vormen.

3. Werkwijze volgens conclusie 2, waarin het aanvullende proces (P*) een cryptografisch proces omvat waaraan een hulpsleutel (K') wordt toegevoerd.

4. Werkwijze volgens conclusie 2 of 3, waarin het aanvullende proces (P*) een inverteerbaar proces is.

5. Werkwijze volgens conclusie 2, 3 of 4, waarin de data (X) tevens aan het aanvullende proces (P*) worden toegevoerd.

6. Werkwijze volgens conclusie 5, waarbij het uitvoeren van het aanvullende proces (P*) uitsluitend plaatsvindt indien de data (X) vooraf bepaalde eigenschappen bezitten.

7. Werkwijze volgens een van de conclusies 2-6, waarin het proces (P) en het aanvullende proces (P*) elk uit een aantal stappen zijn opgebouwd, en waarin afwisselend stappen van het proces (P) en het aanvullende proces (P*) worden uitgevoerd.

8. Werkwijze volgens een van de voorgaande conclusies, waarin het proces (P) een aantal trappen (S) omvat met elk een cryptografische bewerking (F) voor het bewerken van uit de data (X) afgeleide rechter data (RD) en een combinatiebewerking (C) voor het met eveneens uit de data (X) afgeleide linker data (LD) combineren van de bewerkte

rechter data (RD') teneinde gemodificeerde linker data (LD') te vormen, en waarin de rechter data (RD), voorafgaand aan de bewerking F, met een primaire hulpwaarde (A) worden gecombineerd.

9. Werkwijze volgens conclusie 8, waarin de bewerkte rechter data (RD'), volgend op de bewerking F, met een secundaire hulpwaarde (B) worden gecombineerd.

10. Werkwijze volgens conclusie 8 en 9, waarin de secundaire hulpwaarde (B) van een trap gevormd is uit de combinatie van de primaire hulpwaarde (A) van de voorgaande trap en de primaire hulpwaarde (A) van de volgende trap.

11. Werkwijze volgens conclusie 8 of 10, waarin, voorafgaande aan de eerste trap (S_1), de rechter data (RD) met de primaire hulpwaarde (A_1) van de eerste trap (S_1) en de linker data (LD) met een additionele hulpwaarde (A_0) wordt gecombineerd.

12. Werkwijze volgens conclusie 11, waarin, onmiddellijk na de laatste trap (S_n), de rechter data (RD_n) met de primaire hulpwaarde (A_n) van de laatste trap en de gemodificeerde linkerdata (LD') met een verdere additionele hulpwaarde (A_{n+1}) worden gecombineerd.

13. Werkwijze volgens een van de conclusies 8-12, waarin alle primaire hulpwaarden (A) gelijk zijn.

14. Werkwijze volgens een van de conclusies 9-13, waarin de primaire hulpwaarden (A) en/of secundaire hulpwaarden (B) telkens vooraf met de respectieve bewerking (F) zijn gecombineerd.

15. Werkwijze volgens een van de conclusies 8-14, waarin het combineren door middel van een exclusief-of-bewerking wordt uitgevoerd.

16. Werkwijze volgens een van de voorgaande conclusies, waarin de data (X) identificatiedata van een betaalmiddel (1) omvatten en de bewerkte data (Y) een gediversificeerde sleutel vormen.

17. Werkwijze volgens een van de voorgaande conclusies, waarin het proces (P) DES omvat, bij voorkeur drievoudige DES.

18. Schakeling (10) voor het uitvoeren van de werkwijze volgens een van de voorgaande conclusies.

19. Betaalkaart (1), voorzien van een schakeling (10) volgens conclusie 17.

20. Betaalterminal (2), voorzien van een schakeling volgens conclusie 18.

1011544

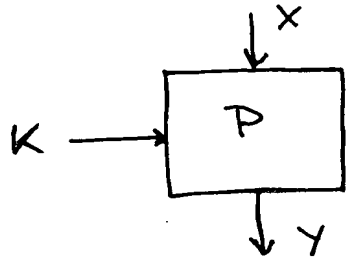

Fig. 1

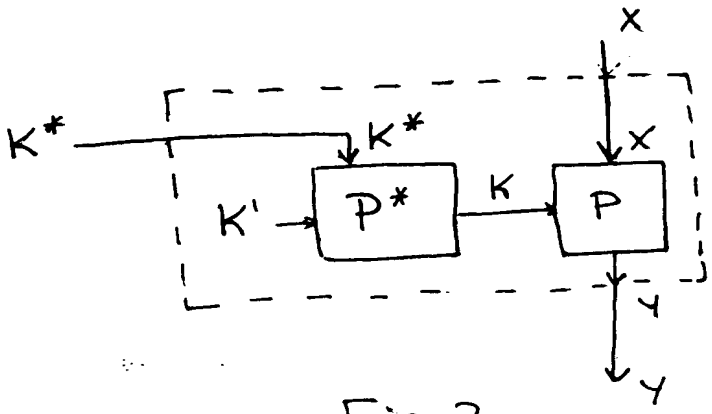

Fig. 2

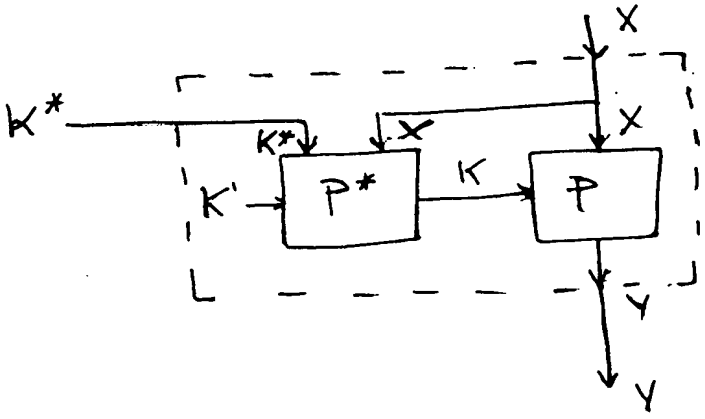

Fig. 3

gm a

1011544

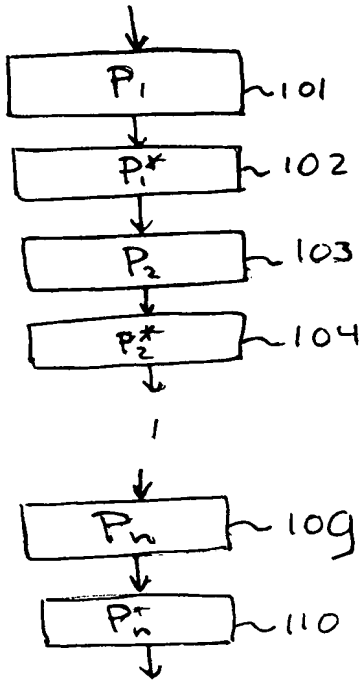

Fig. 4

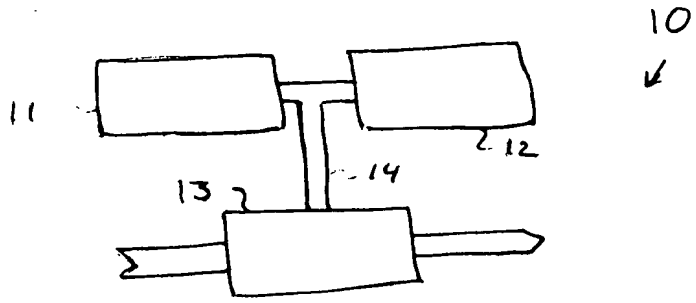

Fig. 8

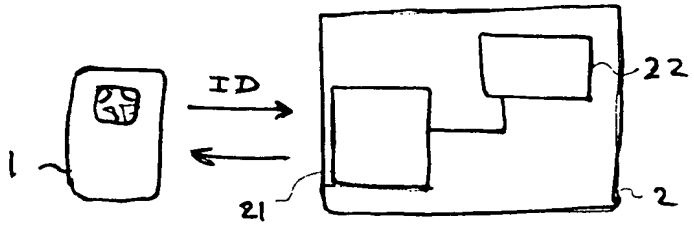

Fig. 9

10 11544

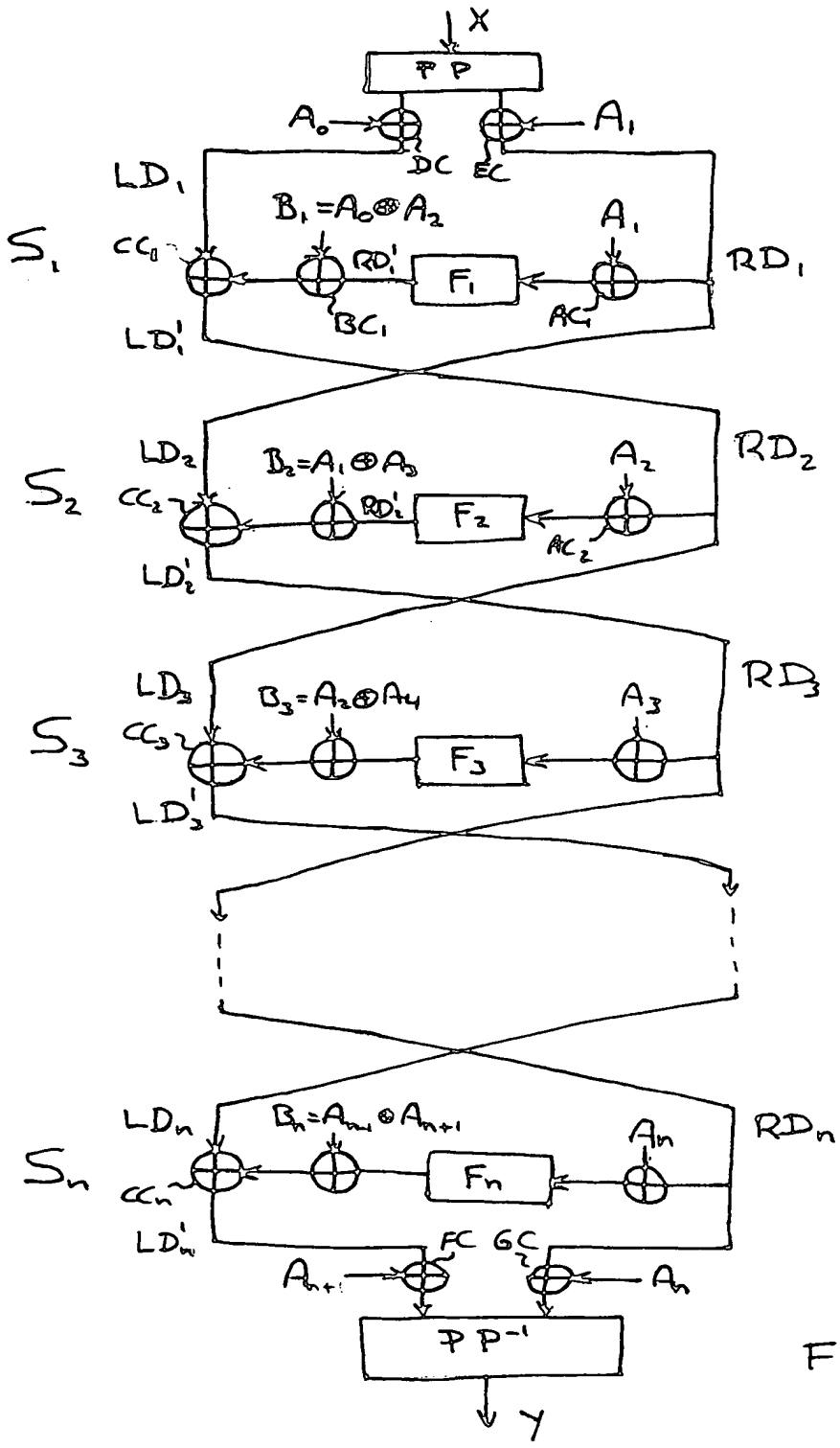

Fig. 5

Got C

1011544

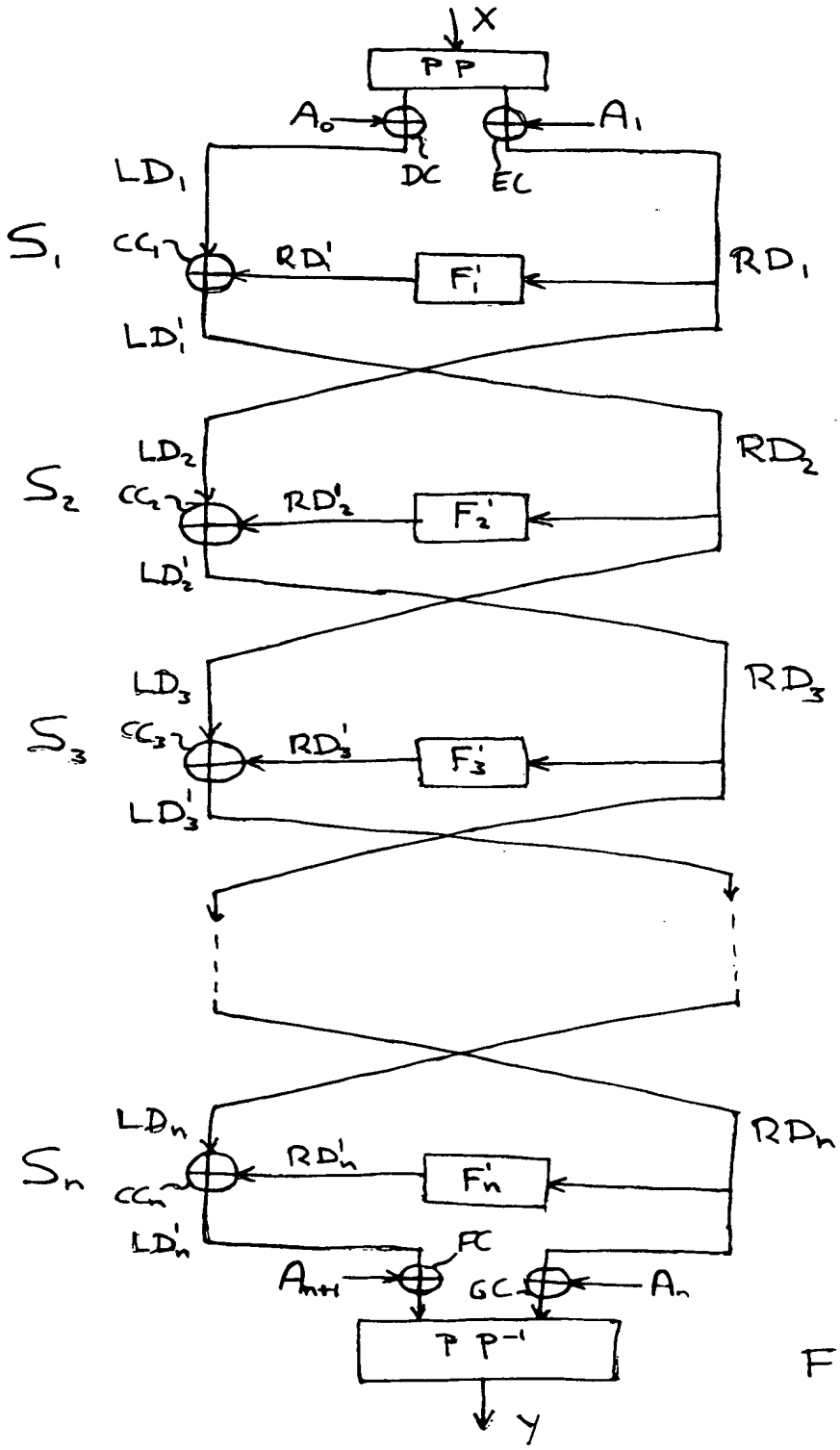

Fig. 6

good

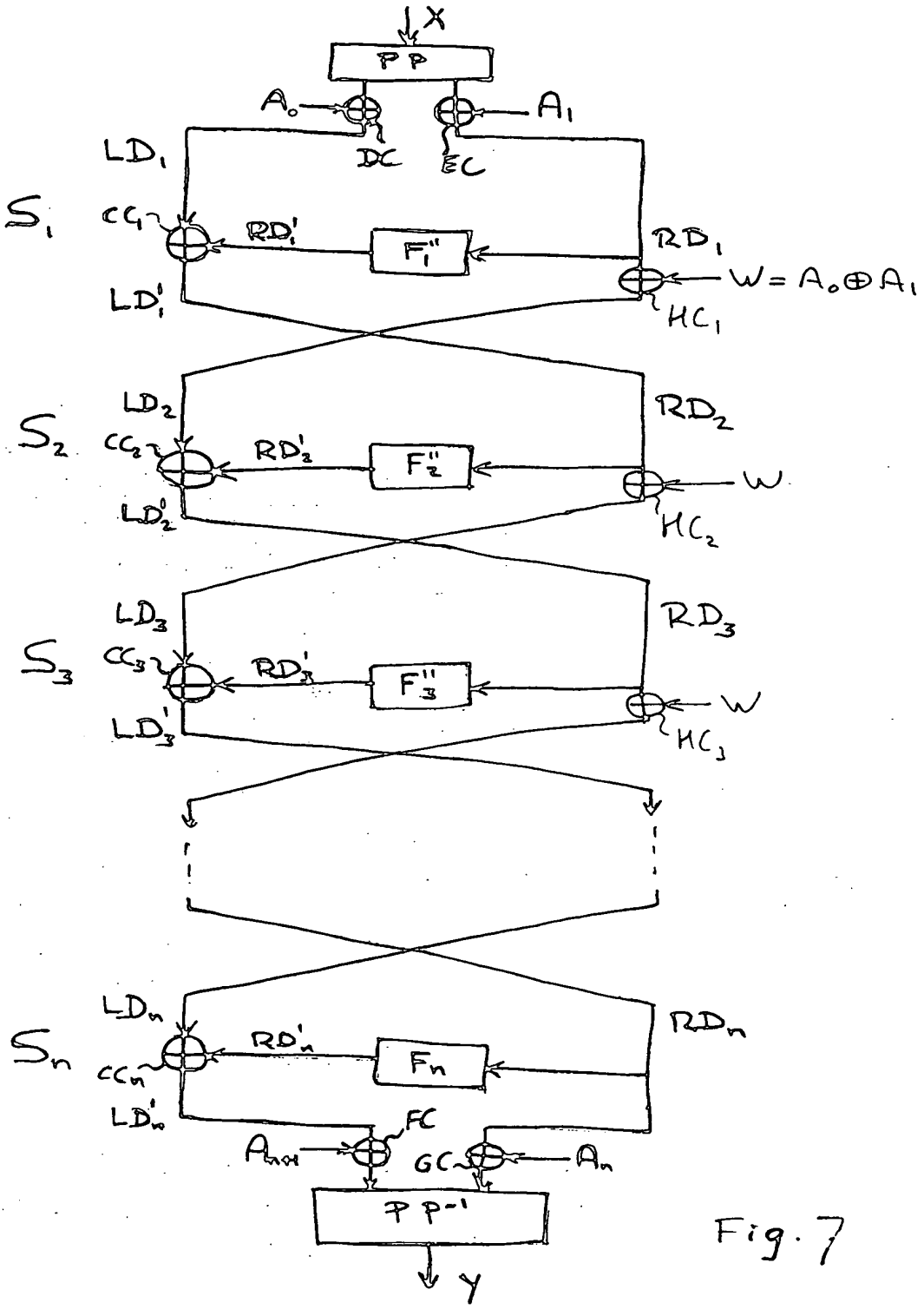
X
PP
A0
A1
DC
EC
LD1
S1
CC1
RD'1
F''1
RD1
W = A0 ⊕ A1
LD'1
HC1
LD2
RD2
S2
CC2
RD'2
F''2
W
LD'2
HC2
LD3
RD3
S3
CC3
RD'3
F''3
W
LD'3
HC3
LDn
RDn
Sn
CCn
RD'n
Fn
LD'n
FC
An+1
GC
An
PP-1
Y

Fig. 7

KINGDOM OF THE (crest) NETHERLANDS

PATENT OFFICE

This certifies that in the Netherlands, on 12 March 1999, a patent application was filed under number 1011544, in the name of:

Koninklijke KPN N.V.

of Groningen

for: "Method and device for cryptographically processing data."

claiming priority of the patent application which was filed in the Netherlands on 30 December 1998 under number 1010921, and that the documents attached hereto are in accordance with the documents originally filed.

Rijswijk, 1 October 1999.

On behalf of the Chairman of the Patent Office,

(signature)

(A.W. van der Kruk)

ABSTRACT

In the event of cryptographically processing data, said data (X) and a key (K) are fed to a cryptographic process (P), which may be a known process. In order to veil the nature of the process (P), there are fed auxiliary values to the process, such as a supplementary key (K*), using which a supplementary process (P*) generates the key proper (K). The combination of the original process (P) and the supplementary process (P*) provides an unknown process, the relationship between the supplementary key (K*) and the processed data (Y) being unknown. As a result, there is obtained an improved cryptographic security.

(FIG. 2)

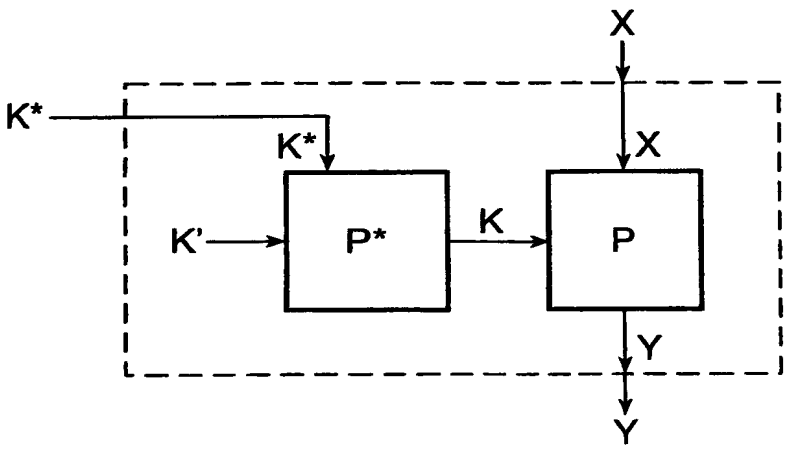

FIG. 2

Method and device for cryptographically processing data.

BACKGROUND OF THE INVENTION

The invention relates to a method for cryptographically processing data, comprising feeding, to a cryptographic process, values, namely, the data and a key, and carrying out the process in order to form cryptographically processed data. Such method is generally known.

For cryptographically processing data, in practice there are often applied generally known processes. Examples of such cryptographic processes (algorithms) are DES and RSA [DES = Data Encryption Standard and RSA = Rivest, Shamir & Adleman], which are described, e.g., in the book ''Applied Cryptography'' by B. Schneier (2nd edition), New York, 1996.

Said processes are published since it was assumed that, in the event of sufficiently large key lengths, it would be impossible, on the basis of the processed data, to retrieve the original data and/or the key, even if the cryptographic process were known.

Recently, however, there were discovered attacks which are based on knowledge of the cryptographic process. In other words, since the behaviour of the process is known, in the event of certain attacks it becomes considerably more simple to derive the key used and/or the original data. It will be understood that such is undesirable.

SUMMARY OF THE INVENTION

The object of the invention is to solve the above problem by indicating a method and circuit, for carrying out a cryptographic process, which render the derivation of the key in the event of application of a known (i.e., public) cryptographic process considerably more difficult or even impossible. For this purpose, a method of the type referred to in the preamble according to the invention is characterised by feeding, to the process, auxiliary values in order to mask the values used in the process.

By masking the date and/or key(s) it becomes considerably more difficult to derive said values on the basis of the behaviour of the process. The result of the process, i.e., the collection of processed data, in the event of a suitable choice

of the auxiliary values may be unchanged, i.e., identical to the result of the process, if no auxiliary values have been fed to it. In this connection, an ''auxiliary value'' is understood to mean a value (data or key) which is fed to the process as a supplement to the corresponding data and key.

The invention is therefore based on the insight that the derivation of the values used in a cryptographic process is rendered considerably more difficult if said values are masked using auxiliary values.

The invention is partly based on the further insight that the use of auxiliary values does not necessarily affect the outcome of the process.

In a first embodiment of the invention, an auxiliary value comprises a supplementary key which is fed to a supplementary process in order to form the key.

By applying a combination of a known process and a supplementary process, there is formed a new cryptographic process, unknown per se, even if the supplementary process is also known per se.

By deriving the key used for the known process (primary key) from a supplementary key (secondary key) using a supplementary process, there is achieved that not the (primary) key of the known process but the supplementary (secondary) key is offered to the combination of processes. In other words, externally the supplementary (secondary) key, and not the real (primary) key of the process proper, is used. Derivation of the key from the original data and the processed data has thereby become impossible. In addition, the derivation of the supplementary key has been rendered seriously more difficult, since the combination of the original process and the supplementary process is not known.

Said embodiment of the invention is therefore based, inter alia, on the insight that the being known of a cryptographic process is undesirable, such contrary to what was so far assumed. Said embodiment is also based on the further insight that attacks which elaborate on knowledge of the process become considerably more difficult if the process is unknown.

The supplementary process preferably comprises a cryptographic process. This renders the derivation of the supplementary key more difficult. Basically, however, a simple

encoding may be applied, e.g., as a supplementary process. In the event of a cryptographic process, there is preferably applied an auxiliary key.

The supplementary process advantageously is an invertible process. This enables the application of the method according to the invention in existing equipment with minimum modifications. If, e.g., a first device gives off a (supplementary) key which is applied in a second device according to the invention, then in the first device there may be used the inverse of the supplementary process to derive the supplementary key from the original key. In other words, although in both the first and the second device internally the original (primary) key is used, there is exchanged, between the devices, the supplementary (secondary) key. Intercepting the supplementary key, however, does not result in knowledge of the original key.

It may be advantageous if carrying out the supplementary process takes place exclusively if the data has predetermined properties. In this manner, cryptographic processing may be carried out for specific, selected data only, while such is blocked for all other data. In this manner, there is achieved a supplementary protection.

An optimum security is provided if the process and the supplementary process are each constructed of several steps and in which there are alternately carried out steps of the process and the supplementary process. As a result, the properties of the known process are further veiled, as a result of which the derivation of the keys is further complicated.

In a second embodiment of the invention, the process comprises several steps, each of which has a cryptographic operation for processing right-hand data derived from the data and a combinatory operation for combining the processed right-hand data with left-hand data derived from the data, in order to form modified data, in which the right-hand data, prior to the operation F, is combined with a primary auxiliary value. As a result, it is possible to mask data used in the cryptographic processing.

The processed right-hand data is preferably repeatedly combined with a secondary auxiliary value. As a result, it is possible to mask the modified left data.

The secondary auxiliary value of a step is advantageously formed from the combination of the primary auxiliary value of the preceding step and the primary auxiliary value of the next step. As a result, it becomes possible to compensate the auxiliary value in the repeatedly next step, as a result of which said auxiliary value will not make itself felt in the end result of the process. A further masking of all data, particularly in the first step, is achieved if the primary auxiliary value of the first step is also combined with the left-hand data.

It is possible to carry out the method according to the invention in such a manner, that all primary auxiliary values are equal. As a result, a very simple practical realisation is possible. The use of several auxiliary values, which are preferably random numbers and are generated anew for each time the process is carried out, however, offers a greater cryptographic security.

A further simplification of said embodiment may be obtained if the primary auxiliary values and/or secondary auxiliary values repeatedly have been combined in advance with the operation in question. This is to say, combining with auxiliary values is processed in the operation in question (e.g., a substitution), in such a manner that the result of the operation in question is equal to that of the original operation plus one or two combinatory operations with auxiliary values. By in advance including in the operation the combinatory operations, a more simple and faster practical realisation is possible.

Said combinatory operations are preferably carried out using an XOR operation [XOR = eXclusive OR]. Other combinatory operations, however, such as binary adding, are basically possible as well.

The invention further provides a circuit for carrying out a method for cryptographically processing data. In addition, the invention supplies a payment card and a payment terminal provided with such circuit.

Below, the invention will be further explained on the basis of the exemplary embodiments shown in the figures.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 schematically shows a cryptographic process according to the prior art.

FIG. 2 schematically shows a first cryptographic process according to a first embodiment of the invention.

FIG. 3 schematically shows a second cryptographic process according to a first embodiment of the invention.

FIG. 4 schematically shows a way in which the processes of figures FIG. 1 and 2 may be carried out.

FIG. 5 schematically shows a first cryptographic process according to a second embodiment of the invention.

FIG. 6 schematically shows a second cryptographic process according to a second embodiment of the invention.

FIG. 7 schematically shows a third cryptographic process according to a third embodiment of the invention.

FIG. 8 schematically shows a circuit in which the invention is applied.

FIG. 9 schematically shows a payment system in which the invention is applied.

PREFERRED EMBODIMENTS

A (cryptographic) process P according to the prior art is schematically shown in FIG. 1. To the process P, there are fed input data X and a key K. On the basis of the key K, the process P converts the input data X into (cryptographically) processed output data Y: $Y = P_K(X)$. The process P may be a known cryptographic process, such as DES (Data Encryption Standard), triple DES, or RSA (Rivest, Shamir & Adleman).

If the input data X and the output data Y are known, it is basically possible to derive the key K used. In the event of a key of sufficiently great length (i.e., a sufficiently large number of bits), it was so far deemed impossible to derive said key, even if the process P were known. Impossible in this case is to say that in theory it is admittedly possible, e.g., by trying out all possible keys, to retrieve the key used, but that such requires an impossibly long computational time. Such ''brute-force attack'' is therefore hardly a threat to the cryptographic security.

Attacks recently discovered, however, make use of knowledge of the process, as a result of which the number of possible keys may be reduced drastically. Deriving the key K used and/or the input data X from the output data Y therefore becomes possible within acceptable computational times.

The principle of the invention, whose object it is to render such attacks considerably more difficult and time-consuming, is schematically shown in FIG. 2. Just as in FIG. 1, to a (known) process P there are fed input data X and a (secret) key K to generate output data Y.

Contrary to the situation of FIG. 1, in the situation of FIG. 2 the key K is fed to the process P from a supplementary process P*. The supplementary process P* has a supplementary (secondary) key K* as input data to produce, under the influence of an auxiliary key K', the (primary) key K as output data. The key K is therefore not fed, as is the case in the situation of FIG. 1, from an external source (e.g., a memory) to the process P, but is produced by the process P* from the supplementary (secondary) key K*:

$$K = P^*_{K'}(K).$$

It is therefore the secondary key K*, instead of the primary key K, which is predetermined and stored, e.g., in a key memory (not shown). According to the invention, the primary key K, which is fed to the process P, is not predetermined.

The auxiliary key K' may be a permanently stored, predetermined key. It is also possible to apply a supplementary process P* in which no auxiliary key K' is used.

The combination of the processes P and P* forms a new process which is schematically designated by Q. To the process Q which, on account of the supplementary process P*, is unknown per se, the input data X and the (secondary) key K* are fed to produce the output data Y. The relationship between the secondary key K* and the primary key K is veiled by the supplementary process P*.

The supplementary process P* preferably is the inverse of another, invertible process R. This is to say:

$$P^* = R^{-1}.$$

This enables producing the secondary key K* from the primary key K using R and the auxiliary key K':

$$K^* = R_{K'}(K),$$

as will be further explained later by reference to FIG. 5. The new process Q may possibly be extended by the process R, in such a manner that the primary key K, instead of the secondary key K*, is fed to the process Q. The primary key K in this case in the process Q is derived from:

$$K = P^*_{K'}(K^*) = P^*_{K'}(R_{K'}(K)).$$

This enables using the same (primary) key as in the prior art.

The cryptographic process according to the invention, schematically shown in FIG. 3, also comprises a process P having a primary key K and a supplementary process P* having an auxiliary key K', the primary key K being derived from the supplementary key K* by the supplementary process P*. Supplementing the process of FIG. 1, in this case the input data X is also fed to the supplementary process P*, in such a manner that the primary key K is determined partly as a function of the input data X:

$$K = P^*_{K'}(K^*,X).$$

As a result, there is obtained a supplementary cryptographic protection. In addition, as a result the possibility is offered to carry out the supplementary process P* exclusively if certain input data is offered. This is to say that the supplementary process P* may comprise a test of the input data X, and carrying out the supplementary process P* may depend on the result of said test. Thus, the supplementary process P*, e.g., may be carried out only if the last two bits of the input data X equal zero. The effect of such an input data-dependent operation is that only for certain input data X the correct primary key K will be produced in such a manner that only said input data will deliver the desired output data Y. It will be understood that as a result the cryptographic security is further enhanced.

FIG. 4 schematically shows the way in which substeps of the processes P and P* may be carried out alternatingly

(''interleaving'') in order to further enhance the protection against attacks. The substeps may include so-called ''rounds'', such as, e.g., in the case of DES. The substeps, however, preferably comprise only one or a few instructions of a program, with which the processes are being carried out.

In a first step 101, there is carried out a first substep P_1 of the process P. Subsequently, in a second step 102, the first substep P_1* of the supplementary process P* is carried out. Likewise, in a third step 103, the second substep P_2 of the process P is carried out etc. This continues until, in step 110, the last substep P_n* of the supplementary process P* has been carried out, it being assumed, for the sake of the example, that the processes P and P* comprise an equal number of substeps. If such is not the case, in step 110 there is carried out the last corresponding substep, and in further steps the remaining substeps are carried out.

By alternating the substeps of the process P, which is known per se, and the process P* (possibly known per se as well), there may be obtained a series of substeps which does not correspond to that of a known process. As a result, the nature of the process is more difficult to recognise.

The cryptographic process schematically shown in FIG. 5 comprises several steps S (S_1, S_2, ...). In each step S, (right-hand) data RD is fed to a cryptographic operation F. Said cryptographic operation itself may comprise a number of substeps, such as an expansion, a combination with a key, a substitution and a permutation. The cryptographic operation F provides processed right-hand data RD', which is combined, in a combinatory operation CC (CC_1, CC_2, ..., the index always indicating the step S in question), with left-hand data LD to form modified (left-hand) data LD' which, just as the original right-hand data RD, is passed on to the next step.

As is shown in FIG. 5, at the end of each step S the modified left-hand data LD' and the right-hand data RD change positions in such a manner that they form the right-hand data RD and the left-hand data LD of the next step.

The left-hand data LD and the right-hand data RD were derived, in a preceding operation PP, from input data X and, in doing so, may undergo a preparatory permutation. The output data of the last step forms the processed data Y of the method,

possibly after it has undergone a final operation, such as an output permutation PP^{-1}.

In accordance with the invention, the data present in and between the steps is masked with auxiliary values. Thus, in any step, e.g., in the step S_2, there is a supplementary combinatory operation AC present which combines the right-hand data RD with a (primary) auxiliary value A before this data is fed to the cryptographic operation F. A supplementary combinatory operation BC is inserted between the cryptographic operation F and the combinatory operation CC with the purpose of combining the processed (right-hand) data RD' with a further (secondary) auxiliary value B. All combinatory operations preferably are XOR operations.

Combining the data LD and RD with the auxiliary values A and B results in the modified data LD' being masked, as a result of which it is considerably more difficult to derive the original data LD and RD from the masked data LD'.

In accordance with a further aspect of the invention, the auxiliary values A and B are related. The second auxiliary value B is formed, preferably using an XOR operation, from the first auxiliary value A_1 of the previous step and the auxiliary value A of the next step:

$$B_i = A_{i-1} \oplus A_{i+1}.$$

This results in each auxiliary value A which, using a further supplementary combinatory operation BC, is combined with the right-hand data RD as an ingredient of the further auxiliary value B, repeatedly being compensated in the next step before the data is subjected to the operation F. The auxiliary value A, however, does make itself felt in the modified data LD', in such a manner that this remains masked between two steps.

The first step S_1 is advantageously preceded by preparatory combinatory operations EC and DC which form the right-hand data RD_1 and the left-hand data LD_1, respectively, of the first step S_1 on the basis of the primary auxiliary value A_1 of the first step and a primary auxiliary value A_0, respectively. Said combinatory operations also preferably are XOR operations. In this case, the combinatory operation AC_1 has the effect of removing the auxiliary value A_1 from the right-hand data RD_1 before offering it to the

operation F_1. In the right-hand data RD_1 which, through crosswise exchange in the second step S_2 will form the left-hand data LD_2, the auxiliary value A_1, and therewith the masking of the data, will be maintained.

The second data SD_1 of the first step S_1 are masked using the additional auxiliary value A_0. By combining with the auxiliary value $B_1 = A_0 \oplus A_2$, the initial auxiliary value A_0 is removed (on account of $A_0 \oplus A_2$ being zero), but the auxiliary value A_2 and the masking achieved by it will be maintained. In this embodiment, the auxiliary value A_0 is advantageously chosen equal to A_1.

In order to remove the auxiliary values prior to the final processing (PP^{-1}), there are foreseen completing combinatory operations FC and GC, which combine the modified left-hand data LD'_n of the last step S_n with an auxiliary value A_{n+1}, and the right-hand data RD_n with an auxiliary value A_n, respectively. As a result, it is possible to carry out the method in such a manner that, notwithstanding the use of the auxiliary values A, the final data Y is equal to that which would be obtained using the conventional method.

Although all auxiliary values A_i are preferably chosen different, with the exception of $A_0 = A_1$, it is possible to choose all auxiliary values A_i equal. In this case, all secundary auxiliary values in the embodiment shown will be equal to zero, so that the further combinatory operations BC may be omitted.

In the process of FIG. 6, which largely corresponds to that of FIG. 5, the combinatory operations AC and BC and the cryptographic operation F are integrated to form a combined operation F'. Integrating the combinatory operations is possible by suitably adjusting, e.g., a substitution table of the operation F. As a result, the supplementary combinatory operations AC and BC may be omitted. Basically, each step S_i requires a different combinatory operation F_i in which various auxiliary values A_i are integrated (see FIG. 5). Only if the auxiliary values A_i are chosen equal, i.e., $A_1=A_2 = \ldots = A_n$, the combinatory operations F_i may be equal.

The embodiment of FIG. 7 largely corresponds to that of FIG. 6. Supplementing FIG. 6, each step S, with the exception of the last step S_n, includes a combinatory operation HC which combines the right-hand data RD with a tertiary auxiliary value

W. The tertiary auxiliary value preferably equals the XOR combination of the auxiliary values A_0 and A_1:

$$W = A_0 \oplus A_1.$$

This results in the operation HC always adding the auxiliary value A_0 and compensating the auxiliary value A_1. As a result, it is possible that all cryptographic operations F are essentially identical, which requires a much smaller processing and/or storage capacity from a processor system with which the method is carried out. It will be understood that, in the embodiment of FIG. 7, the operations F" are adjustments of the original operations F, such that these are corrected for the auxiliary value A_1 and in addition combine the auxiliary value A_0 with their result. In other words, if RD $\oplus$ A_1 is fed to F", the result will equal F" (RD) $\oplus$ W.

FIG. 8 schematically shows a circuit 10 for implementing the method according to the invention. The circuit 10 comprises a first memory 11, a second memory 12 and a processor 13, the memories 11 and 12 and the processor 13 being coupled using a data bus 14. By providing two memories, it is possible each time to carry out a substep of one of the processes P and P* (see FIG. 4), to store the result of said substep in, e.g., the first memory 11, and from the second memory 12 to transfer a previous interim result from the other process to the processor 13. In this manner, it is possible to efficiently carry out the alternating computation of substeps of two different processes.

The payment system schematically shown in FIG. 9 comprises an electronic payment means 1 and a payment station 2. The electronic payment means 1 is, e.g., a so-called smart card, i.e., a card provided with an integrated circuit for storing and processing payment data. The payment station 2 comprises a card reader 21 and a processor circuit 22. The processor circuit 22 may correspond to the circuit 10 of FIG. 5.

At the beginning of a transaction, the payment means 1 transmits an identification (card identification) ID to the payment station 2. By reference to said identification, the payment station 2 determines a key which will be used for said transaction. Said identification ID may be fed as input data X (see the figures 1-3) to a cryptographic process which, on the basis of a master key MK, produces an identification-dependent

transaction key K_{ID} as output data Y. In accordance with the invention, for this purpose the process shown in the figures FIG. 2 and 3 is used, the master key MK having been converted in advance, using a process R, into a supplementary master key MK*. Said supplementary master key MK* is now fed, preferably together with the identification ID, in accordance with FIG. 3, to the supplementary process P* in order to reproduce the original master key MK and to derive the transaction key K_{ID} from the identification ID.

Although, in the figures FIG. 2 and 3, there is always shown one single supplementary process P*, there may possibly be used several processes P*, P**, P***, ... in series and/or in parallel to derive the primary key K.

It will be understood by those skilled in the art, that many modifications and amendments are possible without departing from the scope of the invention.

CLAIMS

1. Method for cryptographically processing data, comprising feeding, to a cryptographic process (P), values, namely, the data (X) and a key (K), and carrying out the process (P) in order to form cryptographically processed data (Y), characterised by feeding, to the process (P), auxiliary values (K*; A, B) in order to mask the values (K; D) used in the process (P).

2. Method according to claim 1, wherein an auxiliary value comprises a supplementary key (K*) which is fed to a supplementary process (P*) in order to form the key (K).

3. Method according to claim 2, wherein the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed.

4. Method according to claim 2 or 3, wherein the supplementary process (P*) is an invertible process.

5. Method according to claim 2, 3 or 4, wherein the data (X) is also fed to the supplementary process (P*).

6. Method according to claim 5, wherein carrying out the supplementary process (P*) takes place exclusively if the data (X) has predetermined properties.

7. Method according to any of the claims 2-6, wherein the process (P) and the supplementary process (P*) each are built up from a number of steps, and wherein steps of the process (P) and the supplementary process (P*) are alternated.

8. Method according to any of the preceding claims, wherein the process (P) comprises a number of steps (S), each having a cryptographic operation (F) for processing right-hand data (RD) derived from the data (X) and a combinatory operation (C) for combining, with left-hand data (LD) also derived from the data (X), the processed right-hand data (RD') in order to form modified left data (LD'), and wherein the right-hand data (RD) is

combined with a primary auxiliary value (A) prior to the operation F.

9. Method according to claim 8, wherein the processed right-hand data (RD') is combined with a secondary auxiliary value (B) following the operation F.

10. Method according to claims 8 and 9, wherein the secondary auxiliary value (B) of a step is formed from the combination of the primary auxiliary value (A) of the preceding step and the primary auxiliary value (A) of the next step.

11. Method according to claim 8 or 10 wherein, prior to the first step (S_1), the right-hand data (RD) is combined with the primary auxiliary value (A_1) of the first step (S_1) and the left-hand data (LD) is combined with an additional auxiliary value (A_0).

12. Method according to claim 11 wherein, immediately after the last step (S_n), the right-hand data (RD_n) is combined with the primary auxiliary value (A_n) of the last step and the modified left-hand data (LD') is combined with a further additional auxiliary value (A_{n+1}).

13. Method according to any of the claims 8-12, wherein all primary auxiliary values (A) are equal.

14. Method according to any of the claims 9-13, wherein he primary auxiliary values (A) and/or secondary auxiliary values (B) have each time been combined with the respective operation (F) in advance.

15. Method according to any of the claims 8-14, wherein combining is carried out using an XOR operation.

16. Method according to any of the preceding claims, wherein the data (X) comprises identification data of a payment means (1) and the processed data (Y) forms a diversified key.

17. Method according to any of the preceding claims, wherein the process (P) comprises DES, preferably triple DES.

18. Circuit (10) for carrying out the method according to any of the preceding claims.

19. Payment card (1), provided with a circuit (10) according to claim 17.

20. Payment terminal (2) provided with a circuit according to claim 18.

ABSTRACT

In the event of cryptographically processing data, said data (X) and a key (K) are fed to a cryptographic process (P), which may be a known process. In order to veil the nature of the process (P), there are fed auxiliary values to the process, such as a supplementary key (K*), using which a supplementary process (P*) generates the key proper (K). The combination of the original process (P) and the supplementary process (P*) provides an unknown process, the relationship between the supplementary key (K*) and the processed data (Y) being unknown. As a result, there is obtained an improved cryptographic security.

(FIG. 2)

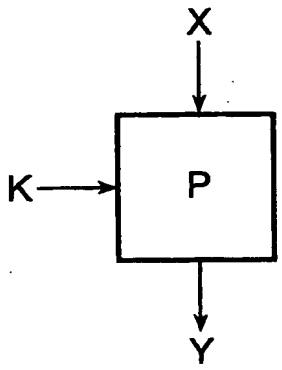

FIG. 1

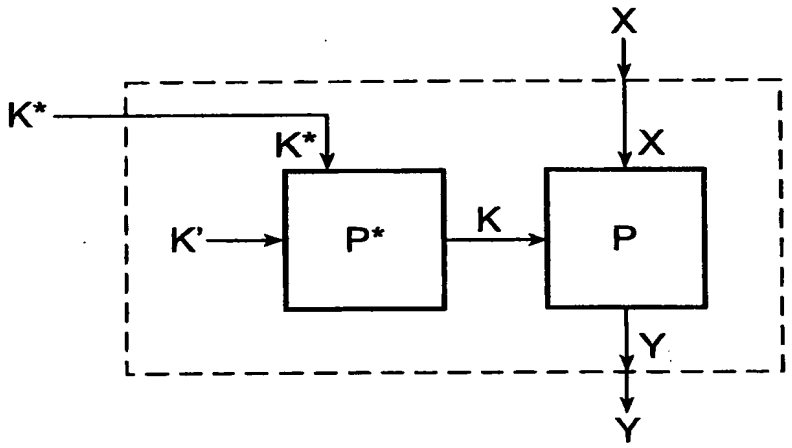

FIG. 2

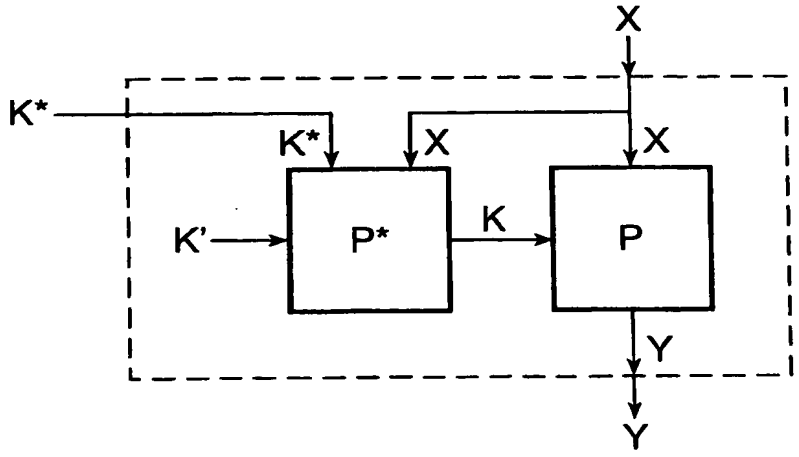

FIG. 3

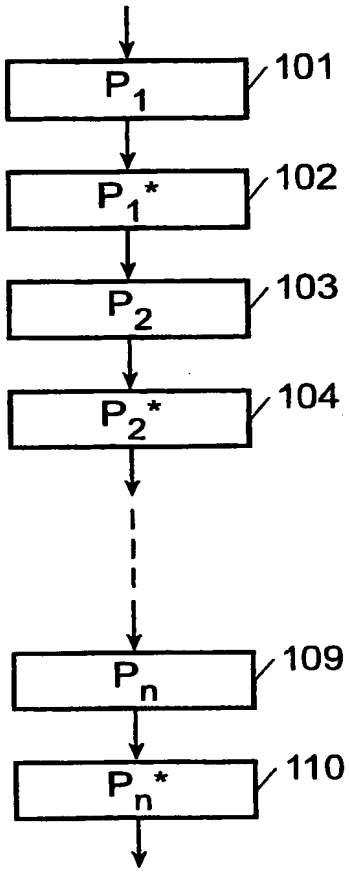

FIG. 4

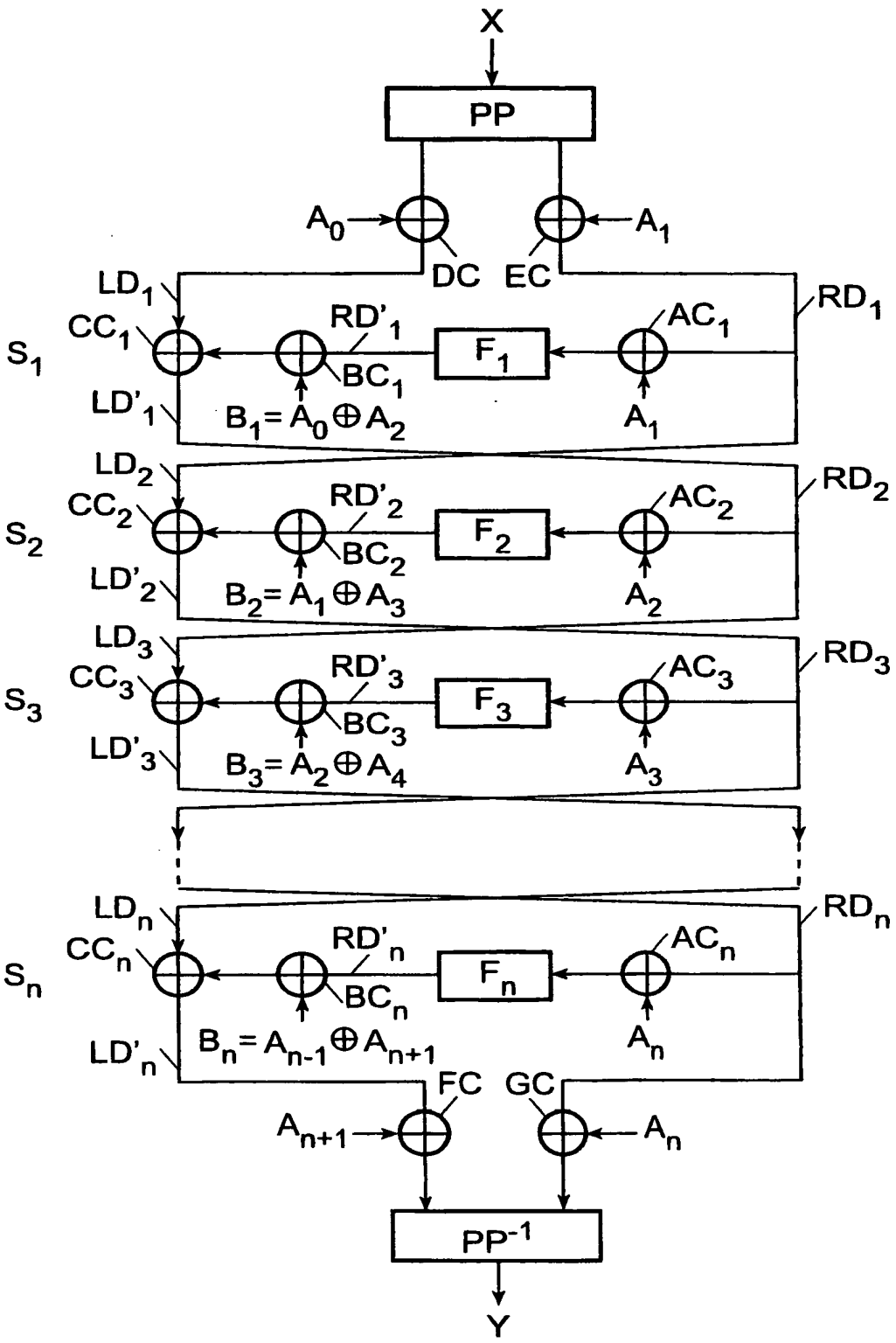
X
PP
A0
A1
DC
EC
LD1
CC1
S1
RD'1
BC1
F1
AC1
RD1
LD'1
B1= A0 ⊕ A2
A1
LD2
CC2
S2
RD'2
BC2
F2
AC2
RD2
LD'2
B2= A1 ⊕ A3
A2
LD3
CC3
S3
RD'3
BC3
F3
AC3
RD3
LD'3
B3= A2 ⊕ A4
A3
LDn
CCn
Sn
RD'n
BCn
Fn
ACn
RDn
LD'n
Bn= An-1 ⊕ An+1
An
FC
GC
An+1
An
PP-1
Y

FIG. 5

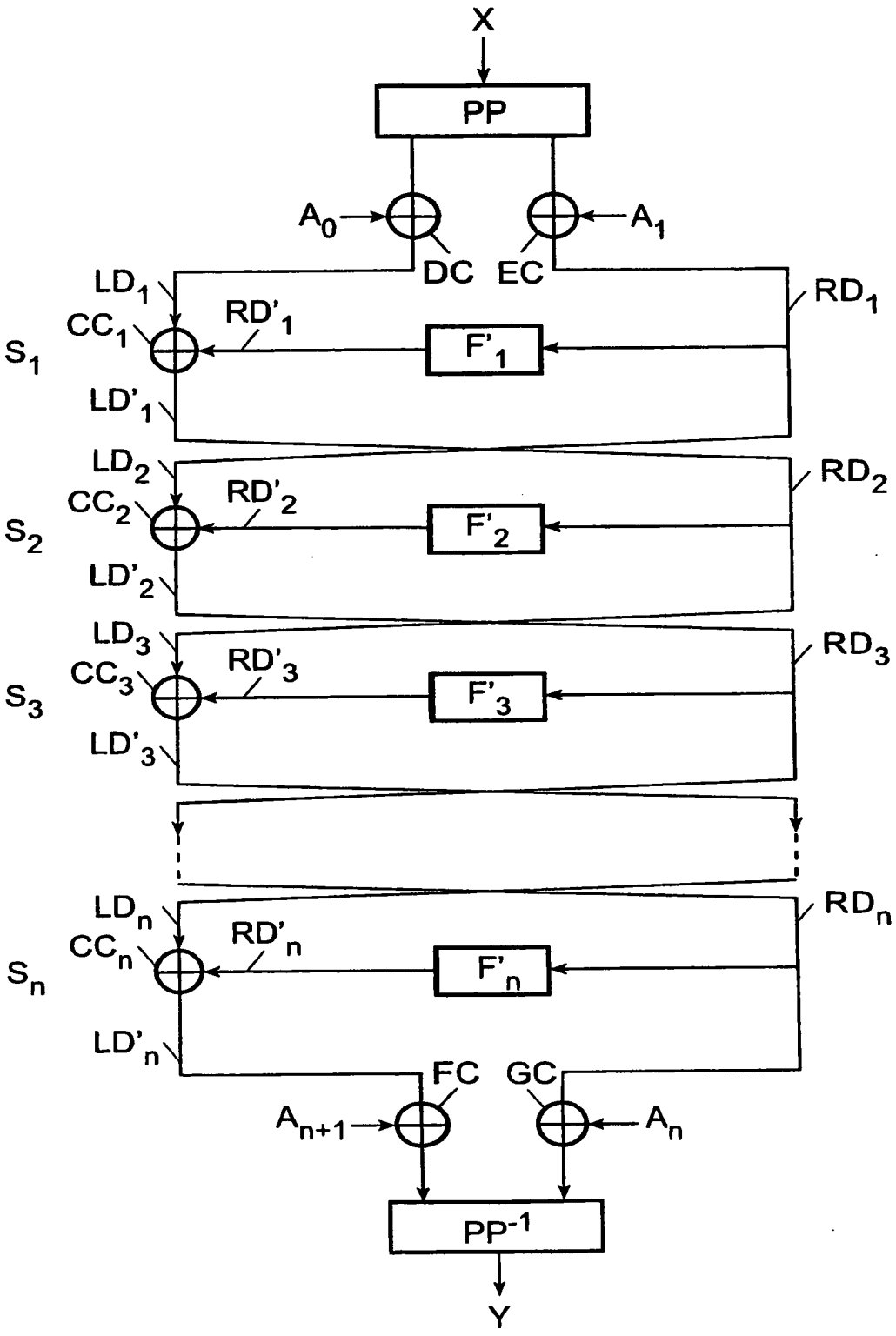
X
PP
A0
A1
DC
EC
LD1
RD1
CC1
RD'1
S1
F'1
LD'1
LD2
RD2
CC2
RD'2
S2
F'2
LD'2
LD3
RD3
CC3
RD'3
S3
F'3
LD'3
LDn
RDn
CCn
RD'n
Sn
F'n
LD'n
FC
GC
An+1
An
PP-1
Y

FIG. 6

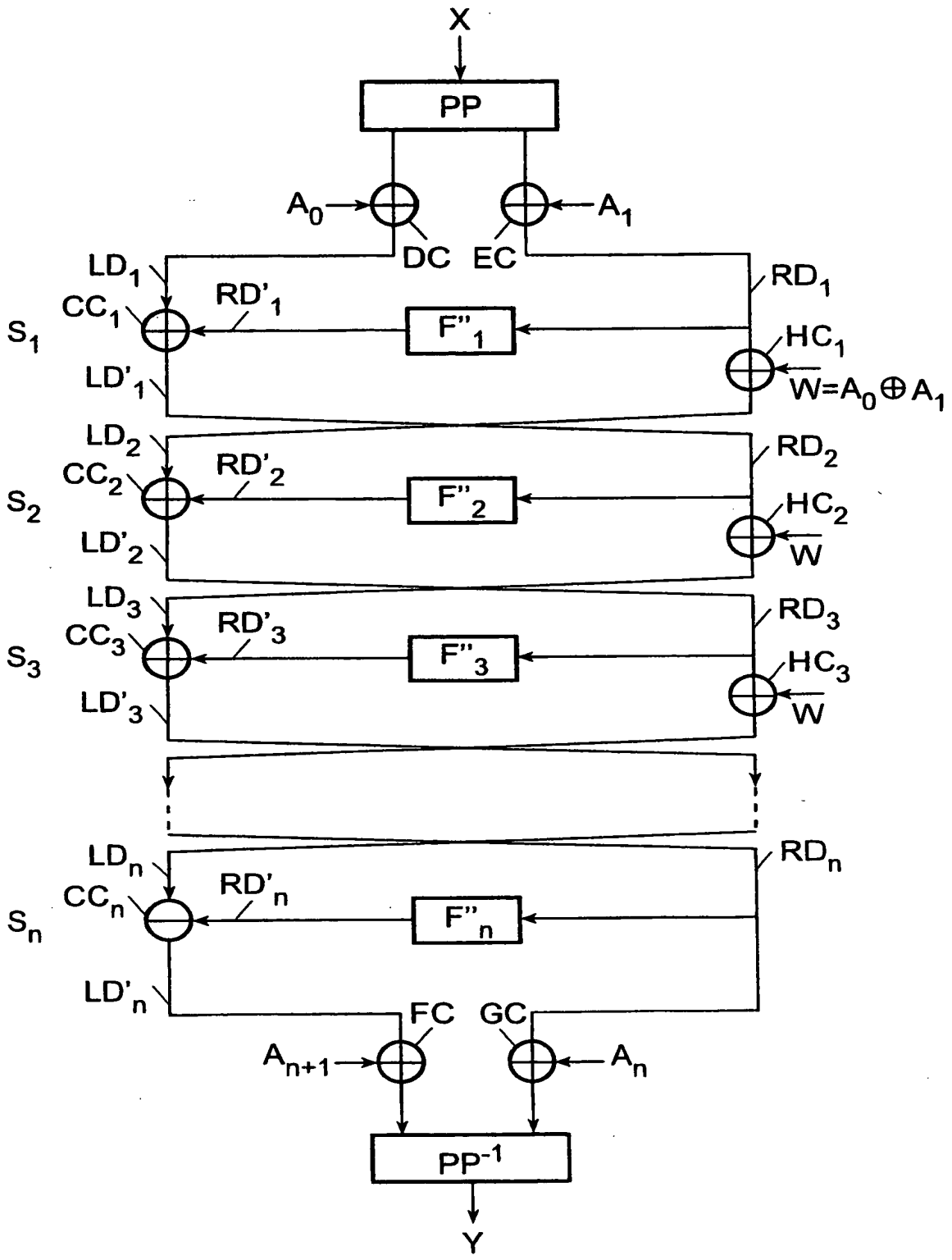
X
PP
A0
A1
DC
EC
LD1
RD'1
CC1
S1
F"1
RD1
HC1
W=A0⊕A1
LD'1
LD2
RD'2
CC2
S2
F"2
RD2
HC2
W
LD'2
LD3
RD'3
CC3
S3
F"3
RD3
HC3
W
LD'3
LDn
RD'n
CCn
Sn
F"n
RDn
LD'n
FC
GC
An+1
An
PP-1
Y

FIG. 7

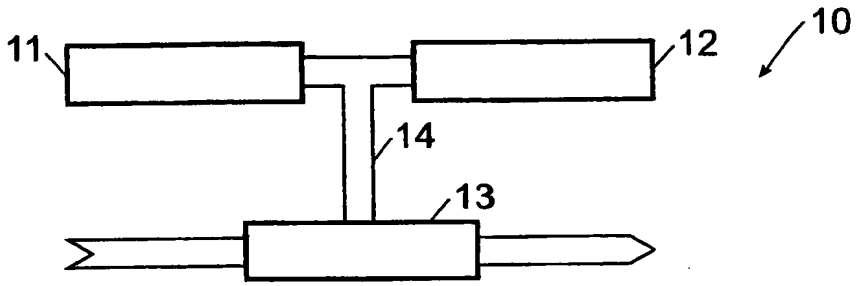

FIG. 8

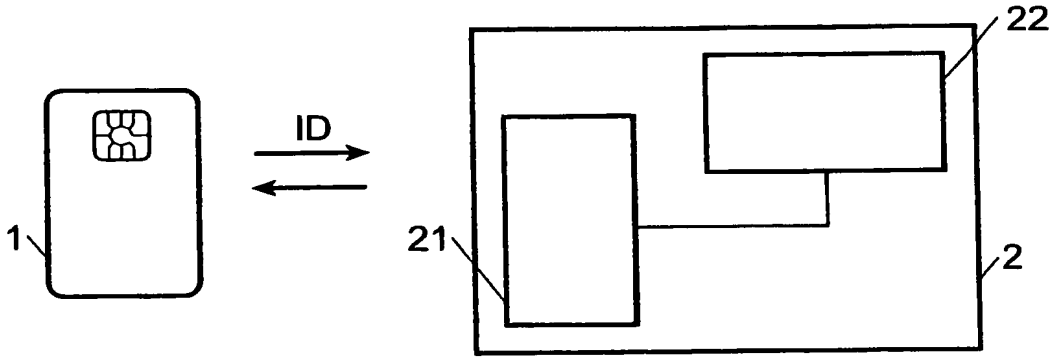

FIG. 9

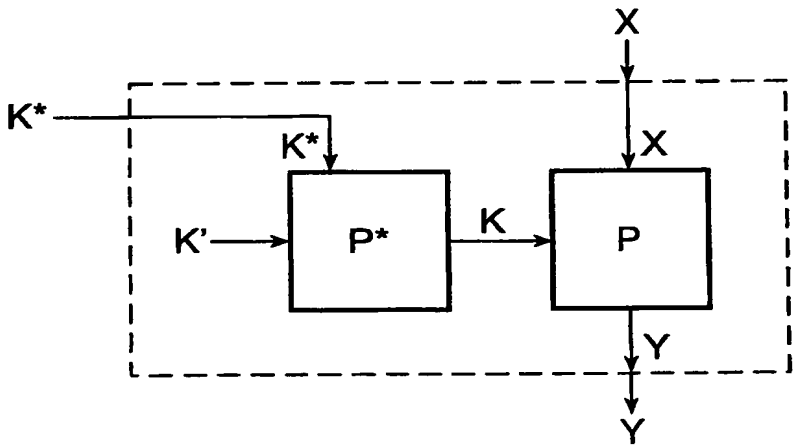

FIG. 2